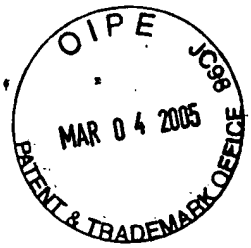
P19949.P11



GREENBLUM & BERNSTEIN, P.L.C.
Intellectual Property Causes
1950 Roland Clarke Place
Reston, VA 20191
(703) 716-1191

AF

Attorney Docket No. P19949

In re application of : Feng BAO et al.

Application No. : 09/623,488 Group Art Unit : 2188

Filed : October 30, 2000 Examiner : P. Parthasarathy

For : A METHOD OF EXCHANGING DIGITAL DATA

Commissioner for Patents
U.S. Patent and Trademark Office
Customer Service Window, Mail Stop _____
Randolph Building
401 Dulany Street
Alexandria, VA 22314

Sir:

Transmitted herewith is an **Appeal Brief Under 37 C.F.R. § 41.37 (in trip.)** in the above-captioned application.

____ Small Entity Status of this application under 37 C.F.R. 1.9 and 1.27 has been established by a previously filed statement.
____ A verified statement to establish small entity status under 37 C.F.R. 1.9 and 1.27 is enclosed.
____ A Request for Extension of Time.
____ No additional fee is required.

The fee has been calculated as shown below:

Claims After Amendment	No. Claims Previously Paid For	Present Extra	Small Entity		Other Than A Small Entity	
			Rate	Fee	Rate	Fee
Total Claims: 11	*20	0	x25=	$	x 50=	$0.00
Indep. Claims: 1	**3	0	x100=	$	x200=	$0.00
Multiple Dependent Claims Presented			+180=	$	+360=	$0.00
Appeal Brief fee				$		$500.00
			Total:	$	Total:	$500.00

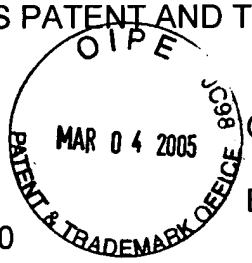
* If less than 20, write 20
** If less than 3, write 3

____ Please charge my Deposit Account No. 19-0089 in the amount of $_____.
__X__ A check in the amount of **$500.00** to cover the filing fee is included.
__X__ The U.S. Patent and Trademark Office is hereby authorized to charge payment of the following fees associated with this communication or credit any overpayment to Deposit Account No. 19-0089.
__X__ Any additional filing fees required under 37 C.F.R. 1.16.
__X__ Any patent application processing fees under 37 C.F.R. 1.17, including any required extension of time fees in any concurrent or future reply requiring a petition for extension of time for its timely submission (37 C.F.R. 1.136(a)(3)).

William Pieprz
Reg. No. 33,630
Bruce H. Bernstein
Reg. No. 29,027

P19949.A10

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE



Appellants	:	Feng BAO et al.	Group Art Unit: 2188
Appln. No.	:	09/623,488	Examiner: P. Parthasarathy
Filed	:	October 30, 2000	
For	:	A METHOD OF EXCHANGING DIGITAL DATA	

APPEAL BRIEF UNDER 37 C.F.R. § 41.37

Commissioner for Patents
U.S. Patent and Trademark Office
Customer Service Window, Mail Stop Appeal Brief
Randolph Building
401 Dulany Street
Alexandria, VA 22314

Sir:

This appeal is from the Examiner's rejection of claims 8-18, as set forth in the Final Official Action of August 4, 2004.

A Notice of Appeal was filed on January 4, 2005 in response to the Final Official Action August 4, 2004, and the two-month period for response was set to expire on March 4, 2005. The requisite fee for filing an Appeal Brief under 37 C.F.R. § 1.17(c) is submitted herewith.

However, if for any reason the necessary fee is not associated with this file or the attached fee is inadequate, the Commissioner is authorized to charge the fee for the Appeal Brief and any necessary extension of time fees to Deposit Account No. 19-0089.

03/07/2005 CCHAU1 00000066 09623488
01 FC:1402 500.00 OP

(1) REAL PARTY IN INTEREST

The real party in interest is Kent Ridge Digital Labs., as established by an assignment recorded in the U.S. Patent and Trademark Office on October 30, 2000, at Reel 011271 and Frame 0640.

(2) RELATED APPEALS AND INTERFERENCES

No related appeals and/or interferences are pending.

(3) STATUS OF THE CLAIMS

Claims 8-18 stand finally rejected. A copy of claims 8-18 is attached as an Appendix to this brief.

(4) STATUS OF THE AMENDMENTS

No amendments to the claims were filed under 37 C.F.R. § 1.116 after the Examiner's final rejection of the claims of August 4, 2004.

(5) SUMMARY OF THE CLAIMED SUBJECT MATTER

Initially, Appellants note that the following descriptions are made with respect to the independent claim and include references to particular parts of the specification. As such, the following are merely exemplary and are not a surrender of other aspects of the present invention that are also enabled by the present specification and that are directed to equivalent structures or methods.

The present invention relates to a method of exchanging digital data between parties over a communication link, and has the advantage of using an off-line trusted third party that does not take part in the exchange unless one of the exchanging parties behaves improperly (Specification, page 5, lines 13-17). The method of exchanging digital data achieves fairness because either the exchanging parties both properly exchange digital data, or no party receives anything useful so that no loss is incurred to a party (Specification, page 5, lines 19-23).

Independent claim 8 requires a method of exchanging digital data over a communications link between a first party having a unique first digital data and a second party having a unique second digital data, the method comprising: the first party encrypting the first digital data and generating an authentication certificate, the authentication certificate authenticating that the encrypted first digital data is an encryption of the first digital data, and sending the encrypted first digital data and the authentication certificate to the second party; the second party verifying that the encrypted first digital data is an encryption of the first digital data using the authentication certificate, and the second party sending the second digital data to the first party when the encrypted first digital data is an encryption of the first digital data; the first party verifying that the second digital data is valid and, when the second digital data is valid, the first party accepting the second digital data and sending the unencrypted first digital data to the second party; the second party verifying that the unencrypted first digital data is valid and, when the unencrypted first digital data is valid, the second party accepting the unencrypted first digital data and, when the unencrypted first digital data is invalid, the second party sending the encrypted first digital data and the second digital data to a third party, the third party having a decryption

key to decrypt the encrypted first digital data; and the third party receiving the encrypted first digital data and the second digital data from the second party when the unencrypted first digital data is invalid, the third party decrypting the encrypted first digital data to obtain the decrypted first digital data, verifying that the decrypted first and the second digital data are valid and, when the decrypted first and the second digital data are valid, sending the decrypted first digital data to the second party and the second digital data to the first party.

In this regard, an exemplary embodiment of the present specification is shown in Figure 1 and disclosed at page 10, line 23 to page 13, line 14. The exemplary embodiment discloses a method of exchanging digital data over a communications link between a first party (A) having a unique first digital data (sign_A) and a second party (B) having a unique second digital data (sign_B), the method comprising: the first party encrypting (step 100) the first digital data and generating an authentication certificate (CEMBS), the authentication certificate authenticating that the encrypted first digital data (C_T) is an encryption of the first digital data, and sending (step 100) the encrypted first digital data and the authentication certificate to the second party; the second party verifying (step 140) that the encrypted first digital data is an encryption of the first digital data using the authentication certificate, and the second party sending (step 180) the second digital data to the first party when the encrypted first digital data is an encryption of the first digital data; the first party verifying (step 200) that the second digital data is valid and, when the second digital data is valid (step 200 = Yes), the first party accepting (step 240) the second digital data and sending (step 240) the unencrypted first digital data to the second party; the second party verifying (step 260) that the unencrypted first digital data is valid and, when the unencrypted first digital data is valid (step 260 = Yes), the second party accepting (step

280) the unencrypted first digital data and, when the unencrypted first digital data is invalid (step 260 = No), the second party sending (step 300) the encrypted first digital data and the second digital data to a third party (T), the third party having a decryption key (SKT) to decrypt the encrypted first digital data; and the third party receiving (step 320) the encrypted first digital data and the second digital data from the second party when the unencrypted first digital data is invalid (step 260 = No), the third party decrypting (step 340) the encrypted first digital data to obtain the decrypted first digital data, verifying (step 340) that the decrypted first and the second digital data are valid and, when the decrypted first and the second digital data are valid (step 340 = Yes), sending (step 360) the decrypted first digital data to the second party and the second digital data to the first party.

(6) GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

(A) Whether Claims 8-18 are properly rejected under 35 U.S.C. § 103(a) over MICALI (U.S. Patent No. 5,666,420) in view of ANGEBAUD et al. (U.S. Patent No. 5,218,637).

(7) **ARGUMENT**

(A) The Rejection of Claims 8-18 Under 35 U.S.C. § 103(a) over MICALI (U.S. Patent No. 5,666,420) in view of ANGEBAUD et al. (U.S. Patent No. 5,218,637) is Improper, and the Decision to Reject Claims 8-18 on this Ground Should be Reversed.

In the Final Official Action of August 4, 2004, 2004, the Examiner rejected claims 8-18 under 35 U.S.C. § 103(a) over U.S. Patent No. 5,666,420 to MICALI in view of U.S. Patent No. 5,218,637 to ANGEBAUD et al. Appellants respectfully submit that the rejection of each of claims 8-18 under 35 U.S.C. § 103(a) over MICALI in view of ANGEBAUD is improper and should be reversed. In this regard, Appellants hereinbelow address the rejection of independent claim 8 and dependent claims 9-18 under 35 U.S.C. § 103(a) over MICALI in view of ANGEBAUD in the numerical order of the claims.

(1) Claim 8

Appellants respectfully submit that even the combination of MICALI or ANGEBAUD does not render obvious at least the above-noted features recited in claim 8, as required for the rejection of claim 8 under 35 U.S.C. §103(a) to be proper. In this regard, Appellants note that, during the course of prosecution of the claims of the present application, the Examiner has shifted her interpretation of MICALI (i.e., the primary reference) from the interpretation provided in the first Official Action dated February 3, 2004. In particular, while the first Official Action applies the teachings of MICALI at col. 5, lines 46-67 and col. 9, lines 50-51 to reject claim 1 (which recited subject matter similar to the subject matter recited in claim 8), the Final Official Action applies the teachings of MICALI at col. 3, line 61

– col. 4, line 28, col. 5, lines 46-62, col. 9, lines 4-14 and 30-61, and col. 11, lines 25-67 to reject claim 8. Further, in an Interview Summary following a personal interview with the Examiner and her Supervisor on September 14, 2004, and in an Advisory Action dated November 30, 2004, the Examiner further applied the teachings of MICALI at col. 3, line 37-col. 4, line 10, col. 5, line 1 to col. 6, line 17, col. 9, lines 4-41 and line 60 – col. 10, line 11, and col. 11, lines 25-67.

Accordingly, because the Examiner has changed her interpretation of at least MICALI throughout the prosecution of the present application, Appellants will first explain the method recited in claim 8 and then compare the method in claim 8 with the entirety of the teachings of the combination of MICALI and ANGEBAUD in order to emphasize the differences between the present invention and the combination of MICALI and ANGEBAUD.

Initially, Appellants would like to explain the invention recited in claim 8 in the context of a non-limiting example. A first party may desire to send a first digital data (e.g., the signature sign_A) to a second party in exchange for a second digital data (e.g., the signature sign_B) from the second party. According to the invention recited in claim 8, the first party encrypts the first digital data and sends the encrypted first digital data (e.g., the encrypted digital signature C_T) to the second party. The first party also generates an authentication certificate that is sent to the second party with the encrypted first digital data. At this time, the second party cannot decrypt the encrypted first digital data. However, the second party can verify that the encrypted first digital data is an encryption of the first digital data using the authentication certificate.

The second party verifies that the encrypted first digital data is an encryption of the

first digital data using the authentication certificate. When the encrypted first digital data (e.g., the encrypted signature C_T) is determined to be an encryption of the first digital data, the second party sends the second digital data (e.g., the signature sign_B) to the first party. However, a problem may arise if the second party then sends invalid or fraudulent data to the first party. Accordingly, the first party verifies that the second digital data is determined to be valid and accepts the second digital data (e.g., the signature sign_B) when the second digital data is valid. When the second digital data (e.g., the signature sign_B) is valid, the first party sends the unencrypted first digital data (e.g., the signature sign_A) to the second party.

The second party verifies the unencrypted first digital data. When the unencrypted first digital data is valid, the process ends because the first and second party are each satisfied. However, if the unencrypted first digital data is invalid, the second party still has the original encrypted first digital data (i.e., which is authenticated as the encryption of the first digital data by the authenticated certificate) from the second party. The second party sends the encrypted first digital data and the second digital data to a third (trusted) party which can decrypt the encrypted first digital data using a decryption key that was used to encrypt the first digital data. Accordingly, the trusted third party can decrypt the encrypted first digital data, verify the decrypted first digital data, and send the decrypted first digital data (e.g., the signature sign_A) to the second party. The trusted third party can also send the second digital data (e.g., the signature sign_B) to the first party.

In other words, each party can verify the data sent by the other party before sending data to the other party. The second party receives an authentication certificate and the first party receives the (unencrypted) second data. Moreover, if a problem arises during the

transaction, the third party assures the fair exchange of the data between the parties.

As is explained below, the outstanding Final Official Action erroneously asserts that the primary reference applied by the Examiner (i.e., MICALI) discloses numerous of the above-noted features recited in claim 8. However, Appellants respectfully submit that MICALI does not disclose or suggest the use of an authentication certificate or that a second party (Bob) verifies (or is able to verify) that the encrypted first digital data is an encryption of the first digital data using the authentication certificate. Rather, MICALI discloses only that Bob receives an encryption "z" of a triplet that includes the message "m", but cannot verify the message "z" as an encryption of the first digital data "m", before signing encrypted message "z" is received and sending the signed encrypted message back to a sender (Alice) as a receipt.

In particular, MICALI discloses, in the Summary of the Invention section, a method of encrypting a data string from a first party to a second party first with a key of the first or second party, and then with a key of the third (trusted) party. The second party digitally signs another data string that is computed from the data string received from the first party. The data string signed by the second party is sent to the first party as a receipt.

In MICALI, if the second party does not eventually get the first value, the second party sends the data string received from the first party to the trusted third party. The third party can decrypt the data string originally sent from the first party to the second party because the data string was encrypted with a key of the third party.

In the Detailed Description, MICALI discloses that the first party is Alice (A), the second party is Bob (B), and the third party is a Post Office (PO). MICALI discloses, at col. 4, lines 66-67, that a first party (Alice) has an identifier "A" and a second party (Bob) has an

identifier "B". For the purposes of this Appeal, Appellants will treat the outstanding Final Official Action as interpreting the "first party" recited in claim 8 as being disclosed by "Alice" in MICALI, as interpreting the "second party" recited in claim 8 as being disclosed by "Bob" in MICALI, and as interpreting the "third party" recited in claim 8 as being disclosed by the "Post Office" in MICALI. A, B and PO can each digitally sign messages and/or encrypt messages using a public-key encryption algorithm (see col. 5, lines 1-18).

MICALI discloses a preferred embodiment at col. 5, lines 37 *et seq*. In the preferred embodiment, Alice computes, at step A1, "z" (i.e., $E_{PO}((A, B, E_B(m)))$), the encryption in the Post Office's public key of a triplet consisting of identifiers A, B, and the encryption of the message "m" with the public key of Bob. As "m" is the data that is encrypted by Alice (and eventually sent in a decryptable format $E_B(m)$ to Bob)), Appellants will treat the outstanding Final Official Action as interpreting the "first digital data" recited in claim 8 as "m" in MICALI. Bob signs "z" at step B1 and sends it to Alice as a receipt. As the signed encryption of "z", i.e., "$Sig_B(z)$", is the only data sent from Bob to Alice, Appellants will treat the outstanding Final Official Action as interpreting the "second digital data" recited in claim 8 as "$Sig_B(z)$" in MICALI.

If Alice receives the properly signed receipt $Sig_B(z)$ from Bob at step A2, then Alice sends Bob the original message "m" encrypted using only Bob's public key (i.e., $E_B(m)$) so that Bob can decrypt the message. Because E_{PO}, A, B, are all public encryptions and identifications, Bob can verify at step B2 that $E_B(m)$, which is received at step A2, corresponds to the same $E_B(m)$ received from $E_{PO}((A, B, E_B(m)))$ at step A1. If Bob cannot verify $E_B(m)$ at step B2, Bob sends the original value "z" to the Post Office, and the Post Office decrypts "z" to obtain $E_B(m)$. Accordingly, Alice receives a receipt for what she sent

to Bob and Bob receives the information $E_B(m)$. Therefore, Alice sends Bob the message $E_{PO}((A, B, E_B(m)))$, and Bob sends Alice a signed receipt for $E_{PO}((A, B, E_B(m)))$.

In practical terms, if the underlying data/message "m" is worthless, Bob has acknowledged receipt of the worthless message "m". However, if the underlying message "m" is valuable, it is only useful to Bob when he provides a receipt for $E_{PO}((A, B, E_B(m)))$ – i.e., he only receives $E_B(m)$ at step A2 when he sends a receipt for $E_{PO}((A, B, E_B(m)))$ at step B1. The remainder of the specification of MICALI is consistent with the above-noted teachings disclosed therein.

In contrast to MICALI, claim 8 recites "the first party encrypting the first digital data and generating an authentication certificate, the authentication certificate authenticating that the encrypted first digital data is an encryption of the first digital data, and sending the encrypted first digital data and the authentication certificate to the second party; the second party verifying that the encrypted first digital data is an encryption of the first digital data using the authentication certificate" (emphasis added). Appellants respectfully submit that MICALI does not disclose or suggest at least the above-noted features recited in claim 8.

In particular, MICALI does not disclose an authentication certificate (or the related features recited in claim 8 anywhere, let alone at those portions of cols. 3, 4, 5 and 9 cited by the Examiner. Further, MICALI merely discloses, at col. 3, line 61 - col. 4, line 27, that a first party and a second party exchange values. Additionally, MICALI discloses, at col. 9, lines 4-41, that digital signatures may be public key signatures, private key digital signatures or signatures verifiable with the help of other parties, or other suitable forms of message authentication. Appellants also note that MICALI discloses, at col. 9, lines 4-41, that the security of a Post Office may be increased by providing a "physically secure

device". However, col. 9, lines 4-41 do not disclose any authentication certificate, let alone the above-noted features recited in claim 8. The above-noted features of claim 8 are also not disclosed in MICALI at col. 9, lines 50-51, which discloses that a Post Office may have a plurality of trustees so that multiple trustees must collude for cheating to occur.

Appellants further submit that MICALI does not use the term "authentication certificate" anywhere, let alone at the above-noted portions of MICALI that were applied in the outstanding Final Official Action. Appellants additionally submit that MICALI does not so much as use the term "certificate" or any equivalent term anywhere, let alone at the above-noted portions of MICALI that were applied in the outstanding Final Official Action.

In the above-noted interview with the Examiner and her Supervisor, the Examiner asserted that the an authentication certificate is inherent in the process of Alice digitally signing a message, as disclosed in MICALI at col. 5, lines 1-3 and col. 6, lines 1-13. Such an interpretation of MICALI is also evidenced in the Interview Summary that was provided following the above-noted interview.

However, Appellants respectfully submit that such an interpretation is incorrect. In this regard, a digital signature is not the same as and does not necessarily invoke an authentication certificate or the features recited in claim 8 that relate to an authentication certificate. Appellants assert that the digital signatures in MICALI are not the same as, and do not necessarily invoke or accompany an authentication certificate or the features recited in claim 8 that relate to an authentication certificate. In this regard, Appellants previously submitted exhibits "A", "B" and "C" with the above-noted Response Under 37 C.F.R. § 1.116, and incorporate the same herein by reference in their entireties. The above-noted exhibits explained the difference between a digital signature and an authentication

certificate. In particular, an authentication certificate is an assertion of the validity of the binding between the certificate's subject (the owner of the cryptographic keys) and her public key such that other users can be confident that the public key does indeed correspond to the subject who claims it as her own. However, a digital signature is a tool for transforming a message by the application of a private key where the data can be verified using the sender's public key. Appellants have further explained that any authentication certificate associated with the issuance of private/public keys could be provided and retained, if provided at all, at a Certification Authority. Thus, the mere use of a digital signature by Alice in MICALI does not disclose, either explicitly or inherently any authentication certificate, let alone features recited in claim 8 that relate to an authentication certificate. Appellants particularly note that the exemplary embodiment of the present application as described above uses an authentication certificate to authenticate that an encrypted digital signature (C_T) is a digital signature (sign_A) of a particular party. Accordingly, the Examiner's interpretation of a digital signature as an authentication certificate is somewhat absurd in the context of the present claims.

Appellants further submit that the Examiner has made additional errors in her interpretation of MICALI as it allegedly relates to claim 8. In this regard, $E_B(m)$ in MICALI is not the encryption of the first digital data of the present invention (i.e., which is not and cannot be decrypted by the second party) since $E_B(m)$ is the message "m" encrypted with Bob's public key (which Bob can easily decrypt). Rather, the encryption of the first digital data in MICALI would be "z", which is $E_{po}(A, B, E_B(m))$, because "z" is not and cannot be decrypted by Bob. However, as noted for step B1 at column 5, lines 50-51, Bob does not verify that "z" is an encryption of the first digital data (i.e., "m") using the authentication

certificate. Rather, Bob merely signs "z" and returns the signed "z" to Alice. Accordingly, MICALI does not disclose "the second party verifying that the encrypted first digital data is an encryption of the first digital data" as recited in claim 8.

Further, MICALI discloses, at column 6, lines 1-5, that Alice can use her secret key to sign "z". Referring to column 5, lines 3-5, the digital signature by Alice on "z" would be $SIG_A(z)$. However, $SIG_A(z)$ is not used by Bob to verify that the encrypted first digital data (i.e., "z") is verified as an encryption of the first digital data (i.e., "m"). Rather, Bob may use Alice's public key to decrypt $SIG_A(z)$ and determine that Alice is the sender (as noted in MICALI at column 6, lines 1-7). Thus, Alice's signature of "z" merely allows Bob to verify the origin of the message and that it has not been modified after Alice signed "z". However, Alice's signature of "z" would not give any assurance to Bob that "z" is necessarily an encryption of the first digital data. In contrast, the authentication certificate of the present invention authenticates that the encrypted first digital data is an encryption of the first digital data. Thus, Alice's digital signature in MICALI does not and cannot obtain the same result for Bob as the authentication certificate recited in claim 8 obtains for the second party.

Accordingly, MICALI does not disclose or suggest that sending "z" to Bob also invokes sending an authentication certificate to Bob. As previously explained, an authentication certificate for private/public keys can be provided at a Certification Authority, and does not require that such an authentication certificate be provided with "z". Further, as previously explained, MICALI does not disclose or suggest that an authentication certificate is provided with "z", particularly because MICALI does not even mention the term "certificate", let alone an "authentication certificate", anywhere in the disclosure thereof.

Accordingly, Appellants respectfully submit that MICALI does not disclose, suggest

or otherwise teach the above-noted features recited in claim 8. In particular, MICALI does not provide any teaching of an "authentication certificate" as in the present invention, let alone an "authentication certificate authenticating that the encrypted first digital data is an encryption of the first digital data", as is recited in claim 8. Furthermore, MICALI does not disclose any feature similar to "the first party... sending the encrypted first digital data and the authentication certificate to the second party", as is recited in claim 8. Moreover, MICALI does not disclose any feature similar to "the second party verifying that the encrypted first digital data is an encryption of the first digital data using the authentication certificate", as is recited in claim 8.

Appellants further submit that the above-noted features are not disclosed or suggested by ANGEBAUD; nor has the Examiner asserted at any time that the above-noted features are disclosed or suggested by ANGEBAUD. Accordingly, because the combination of references applied by the Examiner do not disclose, suggest or render obvious the features recited in claim 8, Appellants respectfully submit that the rejection of claim 8 is inappropriate.

Accordingly, Appellants respectfully submit that MICALI (as well as the combination of MICALI and ANGEBAUD) does not disclose or suggest the above-noted features of claim 8. Appellants further submit that no other reference applied in the outstanding Final Official Action discloses or suggests such features; nor has the Examiner asserted that any other reference discloses or suggests such features. Appellants further submit that there has been no assertion, let alone a showing, of any motivation in the prior art to modify MICALI to obtain the above-noted features recited in claim 8.

(2) Claims 9-18

Appellants additionally submit that claims 9-18 are allowable, at least for the reason that these claims depend from claim 8, respectively, and because these claims recite additional features that further define the present invention. Appellants further submit that claims 9-18 are separately patentable over MICALI in view of ANGEBAUD, which fails to disclose or render obvious, in the claimed combination, *inter alia*,

(i) the first and second digital data are on files M_A and M_B respectively, the first party encrypting the first digital data on a concatenation of file M_A and a one-way hash of file M_B; and, when the encrypted first digital data is an encryption of the first digital data, the second party encrypting the second digital data on a concatenation of file M_B and a one-way hash of file M_A (claim 9);

(ii) the first and second digital data are digital signatures belonging to the first and second party, respectively (claim 10);

(iii) wherein the second digital data is a secret file M which the first party wishes to receive from the second party in exchange for the first digital data (claim 11);

(iv) wherein the first party has a pair of public/private keys in a first digital signature scheme; the second party has a pair of public/private keys in a second digital signature scheme; and the third party has a pair of public/private keys in a public key encryption scheme (claim 12);

(v) wherein the digital signature schemes are discrete logarithm based schemes; and the public key encryption scheme is a discrete logarithm based scheme (claim 13);

(vi) wherein the digital signature schemes are Guillou-Quisquater type digital signature schemes; and the public key encryption scheme is a discrete logarithm based

scheme (claim 14);

(vii) wherein the first and second digital data are digital signatures belonging to the first and second party, respectively (claim 15);

(viii) wherein the first party has a pair of public/private keys in a first digital signature scheme; the second party has a pair of public/private keys in a second digital signature scheme; and the third party has a pair of public/private keys in a public key encryption scheme (claim 16);

(ix) wherein the first party has a pair of public/private keys in a first digital signature scheme; the second party has a pair of public/private keys in a second digital signature scheme; and the third party has a pair of public/private keys in a public key encryption scheme (claim 17);

(x) wherein the first party has a pair of public/private keys in a first digital signature scheme; the second party has a pair of public/private keys in a second digital signature scheme; and the third party has a pair of public/private keys in a public key encryption scheme.

Claim 9

With respect to the rejection of claim 9, Appellants note that the Examiner cites the teachings of MICALI at col. 5, lines 58-59 and col. 8, lines 51-68. However, col. 5, lines 58-59 are directed to step B2 as described above, and relate only to Bob receiving and decrypting $E_B(m)$ to obtain "m". This decryption by Bob is performed using Bob's decryption key because $E_B(m)$ was encrypted using Bob's (public) key to encrypt "m". Accordingly, there is no suggestion at col. 5, lines 58-59 that "m" was encrypted by Alice using "a concatenation of file M_A and a one-way hash of file M_B". Further, there is no

suggestion at col. 5, lines 58-59 that Bob responds to Alice following step B2, let alone that Bob responds by encrypting second digital data "on a concatenation of file M_B and a one-way hash of file M_A". Further, the above-noted features recited in claim 9 are not disclosed at col. 8, lines 51-68 of MICALI, which discloses only that a message "M" may be encrypted by actually encrypting a message and a one-way function of the message.

Claims 10 and 15

Moreover, the Examiner asserts that MICALI discloses the features of claim 10 at col. 4, line 66 and col. 3, line 62-63 and col. 4, lines 14-34. However, as noted above, the first digital data recited in the present claims might only be considered "z" in MICALI, as "z" is the only data that is encrypted by Alice in a way that Bob cannot decrypt (i.e., at step A1). While MICALI discloses that Alice can sign "z" before sending it to Bob, and that Bob signs "z" at B1, there is no disclosure that the data "z" is itself a digital signature (i.e., which is then encrypted and sent to Bob).

Claim 11

Additionally, with respect to the rejection of claim 11, MICALI explicitly discloses that the file from Bob should be a "receipt" for the message "m". In this regard, the Examiner asserts that because ANGEBAUD discloses that the second digital data is a secret file, it would be obvious to modify MICALI for use in an exchange of first digital data for the secret file. However, MICALI explicitly emphasizes repeatedly that the teachings therein are contemplated only for use where a first party want to fairly obtain a receipt (e.g., for an electronic transaction or for certified mail). Accordingly, MICALI does not suggest

anywhere that the receipt should be provided in the form of a "secret" file, and moreover only discloses that the "receipt" is provided by Bob when Bob digitally signs "z".

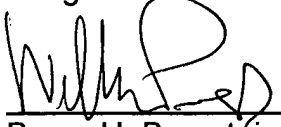
Accordingly, for each and all the above reasons, Appellants submit that the rejection of claims 8-18 under 35 U.S.C. § 103(a) is inappropriate and unsupported by the proposed combination of MICALI and ANGEBAUD et al. Therefore, Appellants respectfully request that the decision of the Examiner to reject claims 8-18 under 35 U.S.C. § 103(a) be reversed, and that the application be returned to the Examiner for withdrawal of the rejection over MICALI in view of ANGEBAUD et al. and an early allowance of claims 8-18 on appeal.

(8) CONCLUSION

Appellants respectfully submit that each and every pending claim of the present application meets the requirements for patentability under 35 U.S.C. § 103, and that the present application and each pending claim are allowable over the prior art of record.

Should there be any questions, any representative of the U.S. Patent and Trademark Office is invited to contact the undersigned at the below-listed telephone number.

Respectfully submitted,
Feng BAO et al.



William Pieprz
Reg. No. 33,630
Bruce H. Bernstein
Reg. No. 29,027

March 4, 2005
GREENBLUM & BERNSTEIN, P.L.C.
1950 Roland Clarke Place
Reston, VA 20191
(703) 716-1191

CLAIMS APPENDIX

Claims 1-7 (Cancelled)

8. (Previously Presented) A method of exchanging digital data over a communications link between a first party having a unique first digital data and a second party having a unique second digital data, the method comprising:

the first party encrypting the first digital data and generating an authentication certificate, the authentication certificate authenticating that the encrypted first digital data is an encryption of the first digital data, and sending the encrypted first digital data and the authentication certificate to the second party;

the second party verifying that the encrypted first digital data is an encryption of the first digital data using the authentication certificate, and the second party sending the second digital data to the first party when the encrypted first digital data is an encryption of the first digital data;

the first party verifying that the second digital data is valid and, when the second digital data is valid, the first party accepting the second digital data and sending the unencrypted first digital data to the second party;

the second party verifying that the unencrypted first digital data is valid and, when the unencrypted first digital data is valid, the second party accepting the unencrypted first digital data and, when the unencrypted first digital data is invalid, the second party sending the encrypted first digital data and the second digital data to a third party, the third party having a decryption key to decrypt the encrypted first digital data; and

the third party receiving the encrypted first digital data and the second digital data from the second party when the unencrypted first digital data is invalid, the third party

decrypting the encrypted first digital data to obtain the decrypted first digital data, verifying that the decrypted first and the second digital data are valid and, when the decrypted first and the second digital data are valid, sending the decrypted first digital data to the second party and the second digital data to the first party.

9. (Previously Presented) The method according to claim 8, in which the first and second digital data are on files M_A and M_B respectively, the first party encrypting the first digital data on a concatenation of file M_A and a one-way hash of file M_B; and, when the encrypted first digital data is an encryption of the first digital data, the second party encrypting the second digital data on a concatenation of file M_B and a one-way hash of file M_A.

10. (Previously Presented) The method according to claim 8, wherein the first and second digital data are digital signatures belonging to the first and second party, respectively.

11. (Previously Presented) The method according to claim 8, wherein the second digital data is a secret file M which the first party wishes to receive from the second party in exchange for the first digital data.

12. (Previously Presented) The method according to claim 8, wherein the first party has a pair of public/private keys in a first digital signature scheme; the second party has a pair of public/private keys in a second digital signature scheme; and the third party has a pair of public/private keys in a public key encryption scheme.

13. (Previously Presented) The method according to claim 12, wherein the digital signature schemes are discrete logarithm based schemes; and the public key encryption scheme is a discrete logarithm based scheme.

14. (Previously Presented) The method according to claim 12, wherein the digital signature schemes are Guillou-Quisquater type digital signature schemes; and the public key encryption scheme is a discrete logarithm based scheme.

15. (Previously Presented) The method according to claim 9, wherein the first and second digital data are digital signatures belonging to the first and second party, respectively.

16. (Previously Presented) The method according to claim 9, wherein the first party has a pair of public/private keys in a first digital signature scheme; the second party has a pair of public/private keys in a second digital signature scheme; and the third party has a pair of public/private keys in a public key encryption scheme.

17. (Previously Presented) The method according to claim 10, wherein the first party has a pair of public/private keys in a first digital signature scheme; the second party has a pair of public/private keys in a second digital signature scheme; and the third party has a pair of public/private keys in a public key encryption scheme.

18. (Previously Presented) The method according to claim 11, wherein the first party has a pair of public/private keys in a first digital signature scheme; the second party has a pair of public/private keys in a second digital signature scheme; and the third party has a pair of public/private keys in a public key encryption scheme.